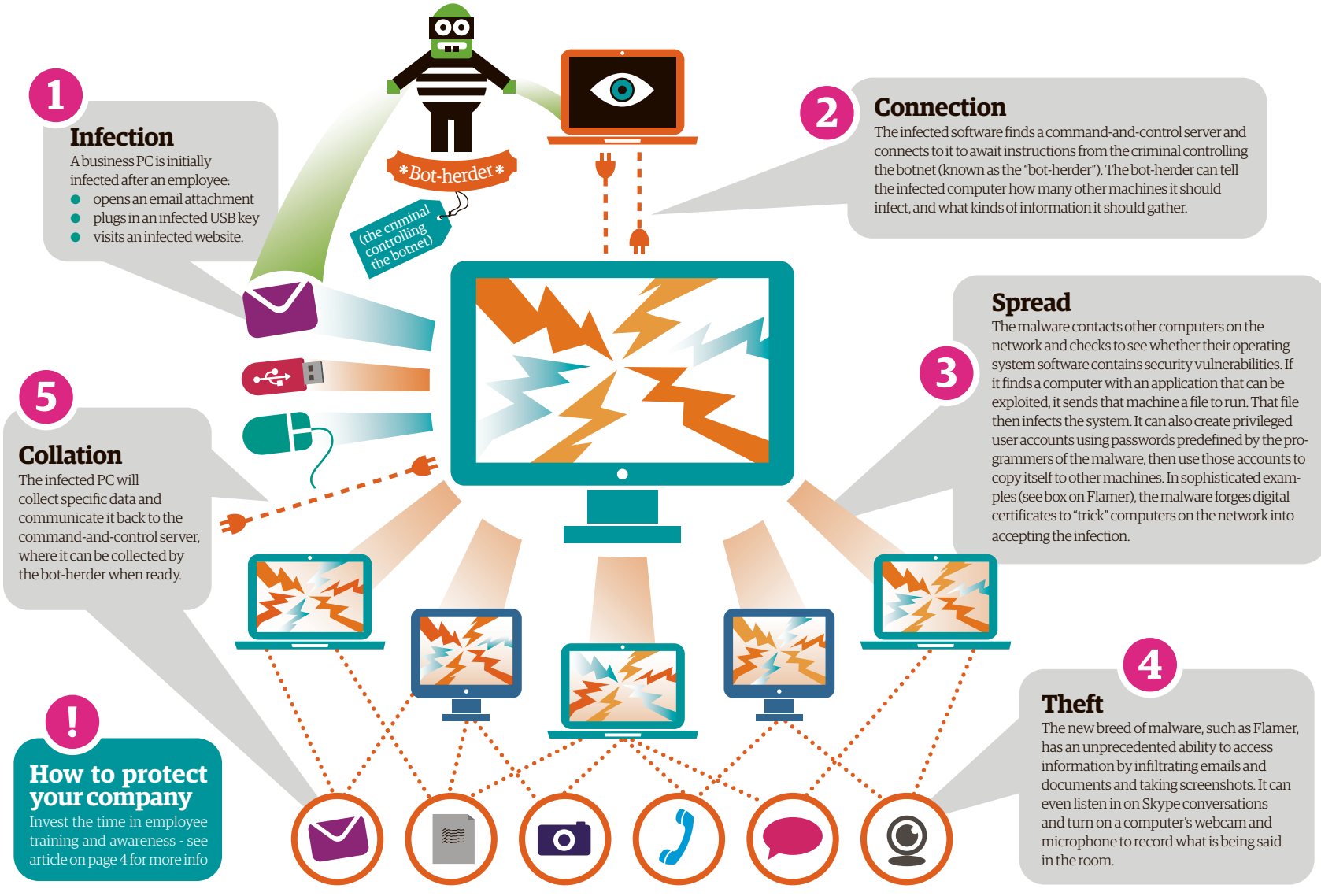
1
Infection
A business PC is initially infected after an employee:
opens an email attachment
plugs in an infected USB key
visits an infected website.
*Bot-herder*
(the criminal controlling the botnet)
2
Connection
The infected software finds a command-and-control server and connects to it to await instructions from the criminal controlling the botnet (known as the "bot-herder"). The bot-herder can tell the infected computer how many other machines it should infect, and what kinds of information it should gather.
3
Spread
The malware contacts other computers on the network and checks to see whether their operating system software contains security vulnerabilities. If it finds a computer with an application that can be exploited, it sends that machine a file to run. That file then infects the system. It can also create privileged user accounts using passwords predefined by the programmers of the malware, then use those accounts to copy itself to other machines. In sophisticated examples (see box on Flamer), the malware forges digital certificates to "trick" computers on the network into accepting the infection.
4
Theft
The new breed of malware, such as Flamer, has an unprecedented ability to access information by infiltrating emails and documents and taking screenshots. It can even listen in on Skype conversations and turn on a computer's webcam and microphone to record what is being said in the room.
5
Collation
The infected PC will collect specific data and communicate it back to the command-and-control server, where it can be collected by the bot-herder when ready.
!
How to protect your company
Invest the time in employee training and awareness - see article on page 4 for more info